

חלק תיאורטי:

ניתוח תקלות רשת ואבטחה:

שאלה: מכונת TEST EC2 לא מצליחה לקבל resolve DNS של כתובות אינטרנטיות, מה הן נקודות הכשל אותן היית בוחן?

תשובה: קודם כל, אני מוודאת שהמכונה רשאית לבקש בקשת DNS. זה נעשה באמצעות חוקים ב-Security Group וב-Network ACL שמאפשרים תנועה יוצאת בפורט 53, שהוא הפורט של DNS. לאחר מכן, אני בודקת שהמכונה יודעת למי לשלוח את בקשת ה-DNS. ב-AWS, זה בדרך כלל ה-VPC Resolver. אם הוא לא מוגדר נכון, הוא לא יודע להביא את התשובה מהאינטרנט.

שאלה: מכונת TEST EC2 מקבלת תרגום כתובות DNS אך נכשלת בתקשורת לאינטרנט (למשל, hub.docker.com ב-443), מה עלול להיות מקור התקלה?

תשובה: אם ה-DNS עובד, זה אומר שיש כתובת IP, אבל הנתונים לא מגיעים ליעד. אני בודקת בטבלת הניתוב של הרשת שהתנועה מכוונת ל-TGW ומשם לרכיב שיודע לצאת החוצה, שזה ה-EGRESS VPC. בנוסף, ה-NFW הוא חומת אש מרכזית. התנועה עוברת דרכו לפני שהיא מגיעה ל-NAT Gateway ויוצאת לאינטרנט. אם אין חוק שמאפשר ל-EC2 לפנות החוצה בפורט 443, ה-Firewall פשוט זורק את החיבור. בנוסף, גם אם כל הניתוב וה-NFW תקינים, ה-Firewall הפרטי של ה-EC2 (ה-Security Group) חייב לאשר את היציאה הזו.

שאלה: על מכונת TEST EC2 מותקן docker engine, repon שלו נמצא ב-ALM VPC במכונת ה-Nexus, מה היית בודק בינתן השגיאות הבאות:

שגיאה 1: pull access denied

תשובה: ה-TEST EC2 הצליח להגיע ל-Nexus, אבל Nexus אמר לו "אין לך הרשאה". אני בודקת אם ה-Login בוצע נכון ואם למשתמש יש הרשאות מתאימות על ה-Repository.

שגיאה 2: container pull time out

תשובה: ה-TEST EC2 ניסה לדבר עם Nexus אבל לא קיבל תגובה בכלל - הנתונים פשוט נעלמו. זה כמעט תמיד חסימת רשת. אני בודקת אם ה-TGW מנתב נכון, ואם חומת האש של Nexus (ה-Security Group שלו) מאפשרת ל-TEST EC2 לדבר איתו בפורט הנכון.

שגיאה 3: docker daemon is not running

תשובה: זו תקלה מקומית לחלוטין. לפני שאני בודקת את הרשת או את Nexus, אני מוודאת שהמנוע (Docker Daemon) בתוך ה-EC2 בכלל פועל, כי אם הוא כבוי, שום פקודת Docker לא תעבוד.

שאלה: החצנת שירות אל מול האינטרנט שמבוסס על רשומת DNS והפניה למכונה TEST EC2. בגישה מבחוץ מקבלים את הכתובת הציבורית של המכונה אך לא מצליחים לגלוש לשירות ב-HTTPS, מה היית בודק ב-flow?

תשובה: ה-Checkpoint FW הוא נקודת המעבר העיקרית לנכנסים. אני בודקת בחוקי הפירורול שלו האם הוא מאפשר חיבור HTTPS לעבור אל TEST EC2, אחרי שה-Checkpoint אישר, החיבור מגיע ל-TEST EC2. עכשיו אני בודקת שהדלת של ה-EC2 (ה-Security Group) פתוחה ל-443 לחיבורים שמגיעים מה-Checkpoint. אם הרשת והחומות אש תקינים, הבעיה היא כנראה אחרת - אני בודקת שהאפליקציה בתוך המכונה מוגדרת לטפל בחיבור HTTPS, ושהתעודה (SSL Certificate) לא פגה או לא מוגדרת נכון.

שאלה: בניסיון ביצוע telnet מהמכונה TEST EC2 מתקבלת שגיאה שתוכנה זו חסרה, איך תתקין אותה על Amazon Linux 2?

מה יכול להיות גורם לכשל ההתקנה שלו מה-repo ובאיזו פקודה היית פותר את זה?

תשובה: בניסיון התקנה לtelnet על Amazon Linux 2, בדרך כלל נהוג להשתמש בyum install telnet, אבל ההתקנה יכולה להיכשל אם השרת לא מצליח להגיע לYUM repositories של אמזון. זה קורה בדרך כלל בגלל בעיית תקשורת החוצה - למשל בעיית DNS, חסימה בSecurity Group או NACL, או מצב שבו השרת נמצא בprivate subnet בלי NAT Gateway. בנוסף, לפעמים גם מטמון של yum גורם לתקלה. במצב כזה, הפתרון הוא לנקות את המטמון בעזרת yum clean all ולהריץ yum makecache כדי לבנות אותו מחדש, ואז לבצע את ההתקנה שוב.

הסבר שלי על התמונה:

שרת TEST EC2 מתחבר לNEXUS EC2 דרך Transit Gateway - שהוא הכלי המרכזי שאחראי לנתב את כל התעבורה בין רשתות VPC השונות. לאחר מכן, כאשר מכונת TEST EC2 רוצה לצאת החוצה לאינטרנט (כמו בפורט 443), התעבורה נשלחת שוב לTGW. TGW מנתב אותה לINSPECTION VPC - שם היא נבדקת על ידי חומות אש מרכזיות (כמו CHECKPOINT FW) המבצעות אבטחה וסינון של בקשות יוצאות ונכנסות. לאחר האישור, התעבורה נשלחת לEGRESS VPC. בEGRESS VPC, התעבורה עוברת דרך רכיבים כמו AWS Network Firewall או NAT Gateway, מגדיר את חוקי התעבורה החוצה לאינטרנט. לבסוף, הTGW מנתב את התעבורה המאושרת אל NAT Gateway, ומשם היא יוצאת החוצה. NAT Gateway מאפשר לסאבנטים פרטיים לצאת לאינטרנט מבלי להישקף לכניסה של בקשות ממנו, ובכך מספק שכבת הגנה נוספת.



